Uwe Krause

(wip) Noch kein Titel

Fakultät Engineering and Computer Science
Department Computer Science

HOCHSCHULE FÜR ANGEWANDTE WISSENSCHAFTEN HAMBURG
Hamburg University of Applied Sciences

Inhaltsverzeichnis

1 Motivation & Einleitung

1.1 Motivation: IT-(un)sicherheit allgemein

- (todo: aktuelle Quelle/Referenz)

1.2 Ziel: Programmierer verbessern

- Unsicherheit „greifbar“ machen
- um für die Einhaltung von „Secure coding Vorgaben“ / „best practices“ zu werben
  - (todo: Referenz??)
- (nicht Pentester ausbilden)

1.3 Didaktische Basis

- Blooms (revisited) Taxonomy [1]
- ICAP (Interactive - Constructive - Active - Passive) [2]

1.4 Vorgehen:

ctf als Elemente aus Pentester-„Ausbildung“ nutzen für Security Awareness bei Programmierern

- ctf as serious game
  - Designing a Serious Game for Cybersecurity Education [3]
  - Software Engineering for Games in Serious Contexts [4]

1.5 Diese Arbeit: Aufbau einer Beispiel-Challenge

In dieser Arbeit wird eine Beispiel-Challenge aufgebaut

1.5.1 Anforderungen an eine Challenge

- On the Requirements for Serious Games geared towards Software Developers in the Industry [5]

1.5.2 Evaluation

- Erfüllungsgrad der Anforderungen
- Vergleich mit anderen CTF
  - (Werte für andere CTF nicht selbst ermittelt: entommen aus Anforderungspaper)

2 Didaktische Basis

Verschiedene didaktische Konzepte bekräftigen, dass Lernende am erfolgreichsten sind, wenn sie sich aktiv mit dem Lerngegenstand beschäftigen.

2.1 Blooms Taxonomie

In Blooms (überarbeiteter) Taxonomie etwa gibt es verschiedene aufeinander aufbauende Ebenen des Verständnis, oft dargestellt als eine Pyramide. Die Basis bildet die Verständnis-Stufe des „Erinnerns“, der Fähigkeit relevantes Wissen aus dem Langzeitgedächtnis abzurufen. Darauf aufbauend folgt das „Verstehen“, das es ermöglicht Wissen zusammenzufassen, zu interpretieren, zu vergleichen und zu erklären. Nach der Stufe des selbst „Anwenden“, steht das Vermögen Sachverhalte zu „analysieren“, also das Material in seine Einzelteile zu zerlegen, übergreifende Struktur und Zweck zu ermitteln sowie Muster zu erkennen. Erst wer dazu in der Lage ist, wird auch „bewerten“ können, sich ein Urteil bilden und Bestehendes kritisieren können. An der Spitze der Taxonomie steht die Fähigkeit angeeignete Elemente zusammenzufügen, um Neues zu erschaffen. [1]

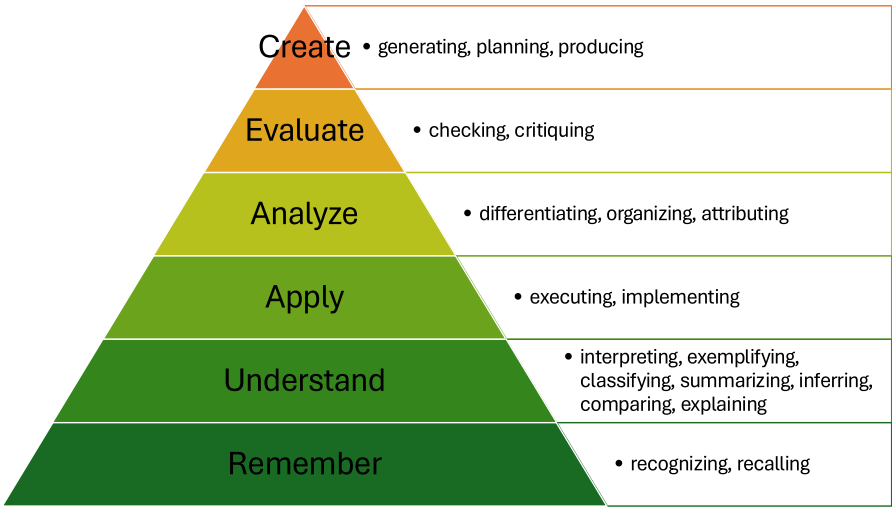

Abbildung 1: Blooms Pyramide, nach [1]. Eigene Darstellung

2.2 ICAP (Interactive - Constructive - Active - Passive)

Bei dem ICAP-Ansatz werden aufbauend auf dem Vorgehensmodell des „aktiven Lernens“ vier Modelle der kognitive Lernaktivitäten definiert und Wege vorgeschlagen, wie Wissensveränderungsprozesse angestoßen werden sollten. Zwar kann Wissen durch das passiven Empfangen von Informationen durch Zuhören oder Lesen aufgebaut werden, dies stellt aber die niedrigste Stufe dar. Die Wissensaufnahme kann aktiver gestaltet werden, zum Beispiel indem beim Zuhören zusätzlich Notizen gemacht werden oder beim Lesen Textstellen angestrichen werden und einzelne Passagen zusammengefasst werden. Konstruktives Verarbeiten ist über die Aufnahme von Erlerntem hinausgehendes Generieren von Dingen, beispielsweise wenn in einer Vorlesung Fragen gestellt werden oder zu einem beschriebenen Zusammenhang eine Zeichnung angefertigt wird. Die höchste Stufe des Modells ist die Interaktion mit dem Lerngegenstand, beispielsweise der Verteidigung eines Standpunkts in einer Gruppendiskussion bei der neue Ideen entstehen. Diesen vier Lernaktivitäten werden die jeweilig zu erwartenden kognitiven Ergebnisse gegenübergestellt: Passiv erlangtes Wissen kann im wörtlich und im gleichen Kontext wiedergegeben werden, wohingegen aktiv Erlangtes auf ähnliche Kontexte angewendet werden kann. Einmal generiertes Wissen kann in neuen Situationen angebracht werden, Kenntnis über das erlernte Konzept erlaubt Interpretation und Erklärungen, auch unter geänderten Rahmenbedingungen. Das tiefste Verständnis ist nach der Interaktion zu erwarten, potentiell können neue Produkte, Interpretationen und Ideen entstehen. [2]

2.3 Methoden der Wissensvermittlung

Die Essenz und das in diversen weiteren Ansätzen immer wieder zu beobachtender Lernmuster, ist die möglichst aktive Beschäftigung mit dem Lerngegenstand durch die Lernenden selbst. [6] Wenn Jura-Studierende Gerichtsurteile aufarbeiten, im Betriebswirtschaftsstudium Fallstudien bearbeitet werden und angehende Mediziner:innen anhand der Begutachtung von Leichen die Todesursache ermitteln [6], wie können Programmierer:innen sich mit den abstrakten Themen der IT-Sicherheit und sichererer Programmierung beschäftigen?

Wird versucht Konzepte der IT-Sicherheit über Vorträge oder Webinare zu IT-Sicherheit zu vermitteln, stellen diese (sofern sie denn überhaupt wahrgenommen werden; ungeteilte Aufmerksamkeit vorausgesetzt) lediglich die niedrigste Stufe der ICAP-Skala dar. Mehr als eine grundlegende Wissensaufnahme ist nicht zu erwarten, was im Bloomschen Modell ebenfalls der untersten Stufe entspricht. Eine aktivere Beschäftigung mit sicheren Programmiermethoden kann etwa bei Code reviews das Hervorheben von fehlerhaftem Code sein. Werden Problembereiche auf diese Art erkannt, entspricht dies dem „Verstehen“ auf der Bloomschen Skala. Es darf erwartet werden, dass das Wissen genug abstrahiert wurde, um eine Chance darauf zu haben, ähnliche Fehler in ähnlichen Kontexten wieder entdecken zu können. Um sich konstruktiv mit IT-Sicherheit zu beschäftigen, bieten sich sogenannte Hackathons an, bei denen Sicherheitsrelevante Systeme oder Komponenten entwickelt werden. Eine Person die bereits einmal etwa ein Login-System entworfen oder implementiert hat, wird benötigte Verfahren nicht nur angewendet haben, sondern wahrscheinlich das Wissen auch in seine Bestandteile zerlegt und zumindest Teile davon analysiert haben. Sie sollte diese Fähigkeit auch unter geänderten Rahmenbedingungen anwenden können. Um die Stufe des tiefsten Verständnis zu erreichen, ist die Interaktion mit einer Sicherheitslücke selbst angebracht, etwa durch das Verteidigen oder Angreifen eines Systems mit einer Sicherheitslücke. Hat eine Angreifer:in es geschafft, eine Sicherheitslücke selbst auszunutzen, hat sie bewiesen das Wissen nicht nur analysiert, sondern auch umfassend bewertet sowie mit dem erfolgreichem Angriff etwas erschaffen zu haben. Und sei dies nur in einer simulierten Umgebung geschehen, so darf trotzdem davon ausgegangen werden, dass das zugrundeliegende Problem wirklich verstanden wurde.

2.4 Serious Games ermöglichen Interaktion

Die skizzierte Form der Interaktion werden auch als „Serious Games“ bezeichnet. Allgemein werden diese entwickelt, um über reale Themen wie Gesundheitsfürsorge, Sicherheit oder Umweltfragen aufzuklären, zu schulen oder zu informieren. [4] Wenn Serious Games das Lernen komplexer und technischer Themen erleichtern, können Konzepte der IT-Sicherheit ebenfalls mit Techniken aus diesem Bereich vermittelt werden. In Lernumgebungen für konkrete zu lernende Konzepte der IT-Sicherheit stellen Spieler sich realistischen Herausforderungen. [3]

Werden auf diese Art IT-Security Techniken vermittelt, findet dies üblicherweise im Rahmen von „capture the flag“ (ctf) statt, einer Art IT-Security-Wettbewerb. Hier gibt es verschiedene Typen von Aufgaben („challenges“), beispielsweise im „Jeopardy-style“, bei dem es für gelöste Aufgaben in unterschiedlichen Kategorien Punkte zu gewinnen gibt. [7] Aufgaben in der Kategorie „Web“ beispielsweise bestehen häufig aus einem Webserver, der den Spielern eine Website mit einer oder mehreren absichtlich platzierten Schwachstellen zur Verfügung stellt. Diesen Webserver gilt es anzugreifen, indem die Sicherheitslücke(n) identifiziert und ausgenutzt werden. Üblicherweise ist zu beobachten, dass Teilnehmende großes Interesse am wettbewerbsorientierten Lernen zeigen [8] und „capture the flag“-Aufgaben die Interaktion von Lernenden mit dem Lerngegenstand erhöhen, was zu besser entwickelten Fähigkeiten im Umgang mit Sicherheitslücken führt [9].

Capture the Flag als Eigenart der Serious Games bieten Teilnehmenden eine Möglichkeit in einer extra hierfür bereitgestellten Umgebungen den Umgang mit Sicherheitslücken zu erlernen. Sie sind also ein geeignetes Mittel, um Kenntnisse im Bereich IT-Sicherheit zu vermitteln.

2.5 Anforderungen an serious games

Damit die eingesetzten Ressourcen möglichst optimal genutzt werden und der Interaktionsgegenstand auf das definierte Ziel einzahlt, müssen die Anforderungen an die Interaktionsumgebung klar formuliert sein. Für Serious Games die sich an praktizierende Software-Entwickelnde richten wurden durch Kombination akademischer und industrieller Forschung 15 Anforderungen[1] definiert. [5]

[1] Die Anforderungen werden gemeinsam mit der folgenden Evaluation in Tabelle 1 aufgelistet.

3 Interaktive Lernumgebung

Im Folgenden wird eine Lernumgebung aufgebaut, die die Interaktion mit einem weit verbreitetem und für Programmierer:innen direkt relevanten IT-Sicherheitsproblem ermöglicht. In diesem serious game besteht die Aufgabe darin eine bewusst platzierte Schwachstelle auszunutzen, was ein tiefes Verständnis für die Problematik fördern soll.

3.1 Lernziele

Teilnehmer:innen sollen diese Sicherheitslücken zukünftig kennen. Sie sollen verstanden haben, dass es Konsequenzen haben wird, wenn eine Angreifer:in diese Lücke ausnutzt. Eigener Code sollte zukünftig frei von diesem Problem sein. Sie sollen in der Lage sein eigenen oder fremden Code daraufhin zu analysieren ob er diese oder eine ähnliche Sicherheitslücke enthält. Sie sollten bewerten, ob verwundbarer Code ausgenutzt werden kann. In einer etwaigen Diskussion sollen sie ihr Gegenüber davon überzeugen können, dass diese Lücke entfernt werden muss.

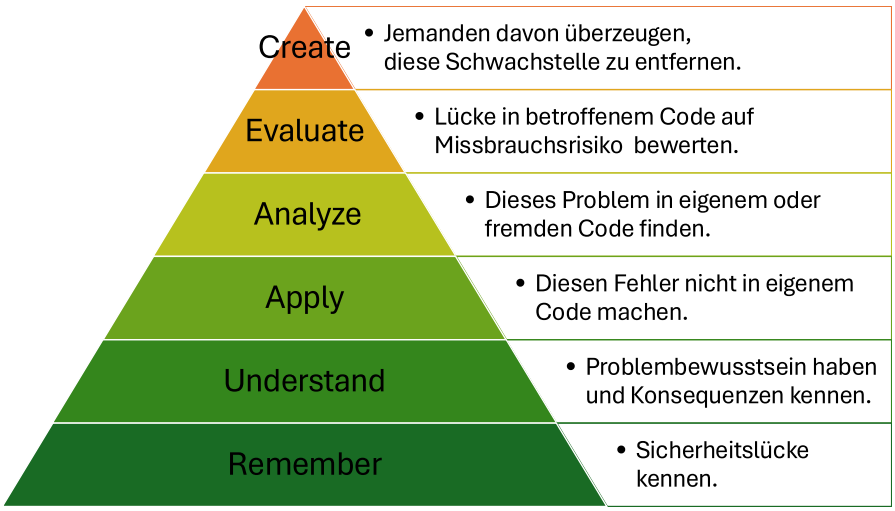

Abbildung 2: Lernziele in Relation zu Blooms Pyramide, nach [1]. Eigene Darstellung

3.1.1 Broken Access Control

Schwachstellen werden von der MITRE-Organisation in einer „Common Weakness Enumeration“-Liste (CWE) gesammelt. [10] In den OWASP „Top 10 Web Application Security Risks“ werden Sicherheitslücken kategorisiert und diese Kategorien werden wiederum nach Inzidenzrate geordnet. [11] Auf Platz 1 der schwerwiegendsten Sicher-

heitsrisiken im Betrachtungszeitraum[2] 2017 – 2021 befinden sich Fehler der Kategorie „Mangelhafte Zugriffskontrolle“. Zugriffskontrollen bezeichnet Mechanismen die sicherstellen, dass Nutzer:innen nur innerhalb ihrer vorgesehenen Berechtigungen handeln können. Werden diese Zugriffskontrollen mangelhaft implementiert, kann eine erfolgreiche Ausnutzung dazu führen, dass eine Angreifer:in Daten unbefugt lesen, ändern oder zerstören kann oder eine Anwendung dazu bringen kann, Dinge zu tun, die die Nutzer:in nicht können sollte. [13]

3.2 Szenario

Die Entstehung der Umgebung soll wenigstens grob der Entstehung einer realen Anwendung folgen. In der anzugreifenden Umgebung soll sich eine fiktive Anwendung befinden, die an und für sich korrekt funktioniert, aber unter Ausnutzung der Sicherheitslücken zu einem (aus Sicht einer fiktiven Organisation) fehlerhaften Verhalten gebracht werden kann.

Für dieses Szenario wird von einer Entwickler:in ausgegangen, die eine Kommunikationsplattform betreiben möchte. Angelehnt an die bestehenden Plattform „Reddit“, bei der sich Nutzer:innen zu vielen verschiedenen Themen öffentlich austauschen können, soll die neue Plattform einen themenbezogenen Austausch in vertraulichen Kleingruppen ermöglichen. Diese Kleingruppen sind im Gegensatz zu Reddit nicht öffentlich, sondern können nur auf Einladung eines Mitglieds betreten werden.

3.2.1 Glesn

Die Entwickler:in kreiert die Konkurrenzplattform „Glesn“[3], welche Anwender:innen verspricht, sich innerhalb eines geschützten „Space“ mit Anderen austauschen zu können. Innerhalb der Spaces können Anwender:innen „Artikel“ schreiben, die von Anderen nur gelesen werden können, wenn diese selbst Teil des Space sind, in dem der Artikel veröffentlicht wurde.

[2] Die nächste Ausgabe der „Top 10 Web Application Security Risks“ wurde für „die erste Jahreshälfte 2025“ angekündigt. [12]

[3] Bayrisch, vulg. für „gelesen“, Anspielung auf „reddit“, was selbst durch ein Wortspiel mit „I read it on reddit.“ entstanden ist [14].

3.2.2 Aufbau der Anwendung

Das User-Interface der Website besteht aus einer Kopf-Bereich und einem Bereich für den anzuzeigenden Inhalt. Der Kopfbereich ist aufgeteilt in einen Unter-Bereich für die Account-Verwaltung und einen Unter-Bereich für die Navigation. Anwender:innen können auf der Seite einen Account anlegen, in dem die Berechtigungen (Zugehörigkeit zu Spaces) hinterlegt sind.

Eine Einstiegsseite erklärt das Prinzip der Seite, also dass Anwender:innen innerhalb geschützter Spaces Artikel anlegen können und dass andere Anwender:innen diese Artikel nur lesen können, wenn sie zuvor von einer Person innerhalb des Space zu diesem eingeladen wurden.

Über die Navigation kann jeweils eine Übersicht aller für den verwendeten Account sichtbaren Spaces und Artikel aufgerufen werden.

Die Artikel bestehen aus einer Überschrift, der Information, welche Autor:in den Artikel verfasst hat, welchen Spaces der Artikel zugewiesen ist und dem eigentlichem Inhalt des Artikels.

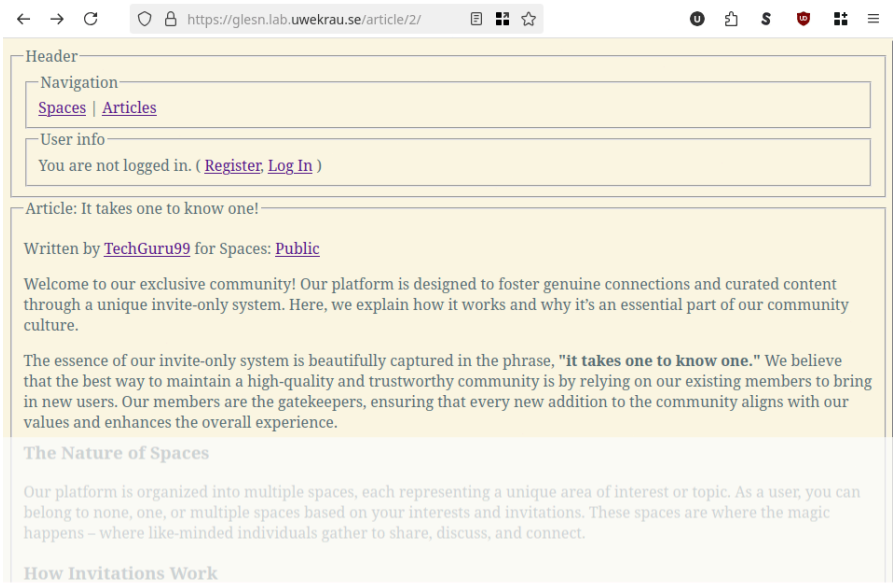

Abbildung 3: Screenshot der Website. In einem öffentlich einsehbareren Artikel wird das Funktionsprinzip erklärt.

Zu einzelnen Autor:innen kann eine Übersicht ihrer Artikel aufgerufen werden. Für angemeldete Anwender:innen besteht außerdem die Möglichkeit, die ausgewählte andere Person zu einem der Spaces einzuladen.

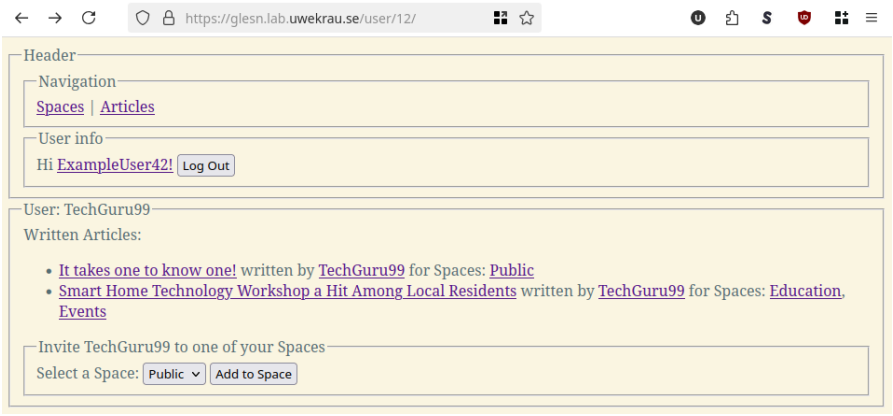

Abbildung 4: Screenshot der Website mit Auflistung der von einer Person verfassten Artikel. Die Person kann zu einem Space eingeladen werden.

3.3 Sicherheitslücken in der Anwendung

3.3.1 Auslesen von Meta-Daten trotz fehlender Zugriffsberechtigung

Programmierer:innen von Web-Anwendungen unterliegen häufig der falschen Annahme, dass die Bedienung nur mit den von der Anwendung selbst bereitgestellten Mitteln möglich ist. [15] Im Beispiel der Glesn-Anwendung werden sowohl in der Spaces-, als auch in der Artikel-Übersicht nur Links zu Ressourcen-Übersichten aufgelistet, auf die die Anwender:in Zugriff hat. Die vergebenen Berechtigungen (Zugehörigkeit zum Space) wird an dieser Stelle respektiert. Über eine direkte Anfrage ist jedoch ein gezielter Zugriff auf die Ressourcen-Übersichtsseite einer ausgewählten Ressource möglich. Wird in der Glesn-Anwendung eine Artikel-Ansicht direkt aufgerufen, wird auch auf der Übersichtsseite noch einmal die Berechtigung überprüft. Der Inhalt des Artikels bleibt also trotzdem geschützt. Die Übersichts-Seite zeigt jedoch Meta-Daten über den Artikel an: Angezeigt werden die Spaces, denen dieser Eintrag zugewiesen ist und die Autor:in des Artikels. Da die Personen-Übersicht nur Artikel anzeigt, zu denen eine Anwender:in Zugriff hat, sich jedoch über den genannten Umweg trotzdem zumindest alle Artikel-Überschriften zu Autor:innen zuweisen lassen, ist dies als Informationsleck [16] zu betrachten.

3.3.2 Rechteausweitung

Wie beschrieben bietet die Anwendung die Möglichkeit, andere Benutzer:innen zu Spaces einzuladen. Durch eine erste Berechtigungsprüfung sind in der grafischen Oberfläche in einer Auswahl-Liste für die Anwender:in nur die Spaces zum Einladen verfügbar, zu

denen Zugriff besteht. Eine Angreifer:in kann die Oberfläche jedoch umgehen und beim Web-Server direkt eine Einladung anfragen. Wieder wird die Annahme ausgenutzt, dass die vom Web-Server angebotenen Endpunkte ausschließlich wie von der Entwickler:in vorgesehen benutzt werden [15]. In der Beispiel-Anwendung wurde davon ausgegangen, dass der Endpunkt durch die erste Berechtigungsprüfung bereits geschützt ist. In diesem Szenario wird deshalb fehlendes Bewusstsein unterstellt, dass vor dem erfolgreichen Aussprechen einer Einladung zu einem Space überprüft werden muss, ob die einladende Person überhaupt selbst über die notwendige Berechtigung verfügt.

Durch die fehlende Autorisationsprüfung werden mehrere Schutzziele der Anwendung gefährdet: Eine Angreifer:in kann eine privilegierte Funktion aufzurufen, die Daten in ihrem Sinne verändert und ihr auf diese Weise Zugriff auf geschützte Informationen liefert. Durch Verletzung der Integrität werden Zugriffskontrollen umgangen und die Vertraulichkeit der Anwendung verletzt. [17]

3.4 Angedachter Lösungsweg der Challenge

Die Challenge lässt sich lösen, indem die innerhalb der Anwendung platzierten Schwachstellen ausgenutzt werden. Die Sicherheitslücken müssen miteinander kombiniert werden, um zum Ziel zu kommen. Es sind aber keine besonderen Angriffswerkzeuge vonnöten, ein üblicher Webbrowser reicht aus. Mit dem Werkzeug der „Netzwerkanalyse“, können in modernen Browsern die einzelnen Aufrufe auf technischer Ebene protokolliert, eingesehen und erneut versendet werden. Einige Web-Browser (z.B. Firefox) erlauben von hier auch vor dem Wiederversenden eine Manipulation der Anfrage.

Als erstes wird davon ausgegangen, dass Angreifer:innen die Anwendung auskundschaften. Hierbei sollte schon ohne Account auffallen, dass die öffentlich sichtbaren Spaces und Artikel anhand ihrer ID aufgerufen werden. Der sichtbare Space „Public“ hat die ID `2` und im Browser wird als Navigationspfad `/space/2/` angezeigt. Der darin abgelegte Artikel hat ebenfalls die ID `2` und wird über `/article/2/` aufgerufen. Die Oberfläche zeigt unter anderem auch einen Link zur Übersichtsseite der Autor:in des Artikels an, die in diesem Beispiel über `user/12/` aufgerufen werden kann. Abbildung 5 zeigt einen Ausschnitt der Netzwerkanalyse.

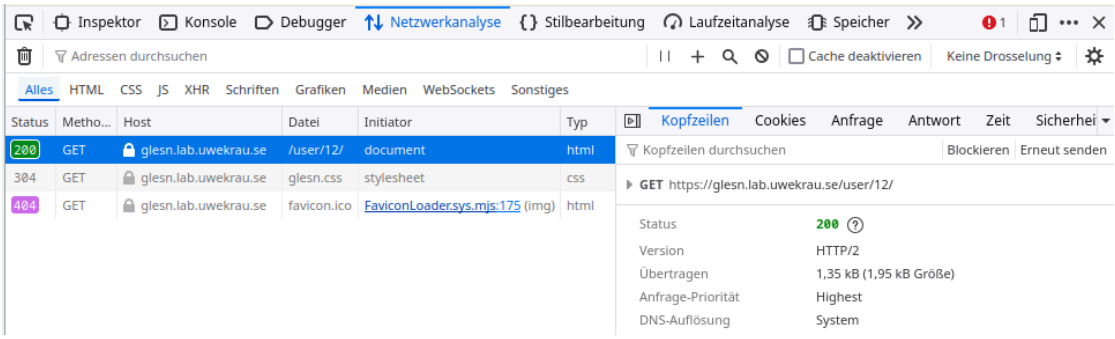

Abbildung 5: Screenshot der Netzwerkanalyse: Erfolgreicher GET Aufruf auf `/user/12/`.

Durch einen direkten Aufruf der Ressourcen, in Kombination mit der Anzeige der unzureichend geschützten Meta-Daten, können weitere Spaces, Artikel und Autor:innen enumeriert werden. Auf diese Weise kann ein Account mit dem Namen „admin“ gefunden werden, ein Space dessen Name im Beispiel „!!! ADMIN ONLY !!!“ lautet und ein Artikel mit der Überschrift „Note FOR ADMINS ONLY !!!“. Das zu erreichende Ziel dürfte deutlich sein.

Nun sollte die nächste zur Verfügung stehende Funktionalität der Website verwendet werden: Die Registration eines neuen Accounts. Mit diesem Account sind zwar keine zusätzlichen Spaces oder Artikel sichtbar, aber auf der Informationsseite zu anderen Autoren erscheint nun die Möglichkeit, andere Personen zu Spaces einzuladen, wie in Abbildung 4 gezeigt. Mit Hilfe der Netzwerkanalyse kann dem Protokoll entnommen werden, dass eine Einladung zu einem Space auf technischer Ebene durch ein `POST`-Request angefordert wird. Dieser Anfrage wird als Argument die ID des Spaces über den Parameter `space_id` übergeben, wie in Abbildung 6 dargestellt.

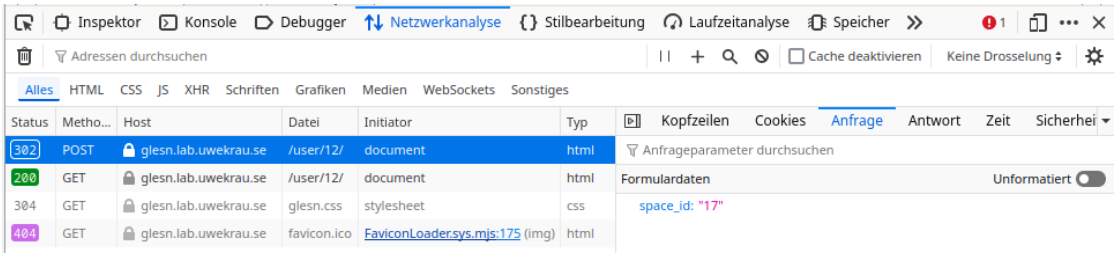

Abbildung 6: Screenshot der Netzwerkanalyse: Erfolgreicher POST Aufruf auf `/user/12/` mit Argument `space_id: "17"`.

Der angedachte Lösungsweg sieht vor, dass eine Angreifer:in nun versuche sollte, die Parameter der Anfrage zu manipulieren und zu probieren, verschiedenen Accounts zu verschiedenen Spaces einzuladen. Aufgrund der Sicherheitslücke der fehlenden Berech-

tigungsprüfung wird dies gelingen und die Angreifer:in kann sich selbst durch eine manipulierte `POST`-Anfrage zu dem Space mit der `space_id: "1"` einladen. Da sie nun Mitglied des Spaces ist, also ihre eigenen Zugriffsrechte erhöht hat, kann sie über die reguläre Benutzeroberfläche auch den Inhalt der Notiz lesen.

3.4.1 Tipps und Hinweise für Lösungsweg

- Der erste Beitrag, der sichtbar ist, hat die ID 2
  - Hinweis darauf, dass es einen Eintrag mit der ID 1 geben müsste.
- Der erste Beitrag (ID 1) ist eine vom (simulierten Admin) angelegte Notiz an andere Admins
  - Der Admin drückt Freude darüber aus, wie einfach das initiale Setup dadurch war, dass das System einfach dem ersten User-Account Administrationsrechte gibt.

3.5 Realitätsbezug

2024 September: KIA

- News
  - Spiegel: Hacker konnten koreanische Autos per App orten, starten, hupen lassen
  - Heise: Kia: Lücken in Webportal erlaubten Forschern Fernzugriff auf Autos
  - Der Standard: Schwere Sicherheitslücken bei Kia ermöglichten Fernortung und Start von Millionen Autos
- Blog (Originalquelle)
  - Sam Curry: Hacking Kia: Remotely Controlling Cars With Just a License Plate

TODO: da werden sich schon noch Beispiele finden lassen

3.6 Beta-Test

Hamburger CTF-Team Cyclopropenylidene (C3H2)

- Feedback: ID für ersten sichtbaren Artikel sollte 2 sein, als Hinweis darauf, dass es einen weiteren Artikel (ID 1) gibt.
  - -> so umgesetzt
- Technisches Problem aufgedeckt: Ein Beta-Tester hat nicht nur einen Account angelegt und diesem (wie angedacht) einen Account Zugriff auf den versteckten Space gegeben, sondern mit Hilfe eines http replay Proxy die Sicherheitslücke so ausgenutzt, dass alle

Accounts Zugriff auf den versteckten Space hatten. das hat dafür gesorgt, dass eine Beta-Testerin, die sich zuvor einen Account angelegt hat, aber die Sicherheitslücke noch nicht gefunden hat, plötzlich ohne eigenes zutun Zugriff auf den versteckten Space hatte.

- -> Gelernt: Diese Challenge muss pro Person/Team als eigene Instanz bereitgestellt werden.

3.7 Durchführung Workshop

- Workshop Week an HAW September 2024
  - ca. 12 Teilnehmende
  - Studierende
    - Informatik
      - Bachelor
      - Master
    - Sonstige
  - Evaluationsbögen
    - TODO: Ergebnis der Evaluationsbügen nutzbar?? (Jedenfalls nicht für direkten Vergleich!) (Eventuell noch ein Workshop notwendig??)

4 Ergebnis

4.1 Evaluation

TODO: Die entstandene Challenge so evaluieren, wie in [5] beschrieben.

- semi-strukturierte Interviews ()
- Feedbackbogen (was hat gut funktioniert, was nicht)
- Fragebogen, Evaluationsfragen

Direkter Vergleich des Ergbenis der EIGENEN Challenge mit den Challenges aus dem Requirements-Paper [5]

Index	Requirement	Evaluation
1	Have a clearly defined learning goal objective	todo
2	Adapted to background (job description) of participants developers	todo
3	Well defined working mechanics (e.g. which tools to use or what to do)	todo
4	Defined and progressive level of difficulty challenges	todo
5	Elicit discussions of the solutions (e.g. is there a better/simpler way to solve?)	todo
6	Provide possible solution after challenge solved	todo
7	Adapted to the skill level of participants	todo
8	Challenge includes hint that aid to arrive to the solution	todo
9	Clear, standardized and simple solution (not based on obscure knowledge)	todo
10	Planned duration of the exercise	todo
11	Explains issues arriving from interplay of different technologies or components	todo
12	Adapted to company internal secure coding guidelines and policies	todo
13	Challenges are put from the defensive perspective	todo
14	Solutions does not require specific knowledge of hacking tools	todo
15	Challenges should raise awareness on possible consequences of malicious attack	todo
		?? %

Tabelle 1: Evaluationsergebnis

- Ergebnis (hoffentlich): meine Challenge erfüllt die Anforderungen besser

4.2 Diskussion

Die Evaluation zeigt, dass

- …?
- Zielgrupopenorientiertheit (zugeschnitten auf Jobtitle) weiterhin schwierig
- … ?

- Challenges are put from the defensive perspective
  - not fulfilled??
- ...?

5 Fazit

. . .

5.1 Ausblick

Durch einen „import“ anderer „Modelle“ aus dem Unterhaltungsbereich könnten „Empfehlungen für Verbesserungen und Erkenntnisse zur Gestaltung und Entwicklung effektiverer SG [Serious Games]“ übernommen werden [18] Die durchgeführte Evaluation sowohl der bestehenden CTF-Events als auch der entwickelten Challenge ist ausbaufähig.

Ein konkretes Beispiel für die Übernahme von bestehenden Methoden aus der Unterhaltungsmedien-Entwicklung könnte ergänzend oder anstelle der durchgeführten Evaluation Evaluations-Methoden aus der allgemeinen Spiele-Entwicklung oder dem Übergeordneten Feld der „serious games“ auch auf die entwickelte/n Challenge/s adaptiert werden. Ansätze hierfür finden sich zum Beispiel in [User Experience Evaluation Methods for Games in Serious Contexts] [19] oder [Framework for evaluating Capture the Flag (CTF) security competitions] [20]

Wird das Feedback der Teilnehmenden ernst genommen und liefern die Evaluations-Methoden gute Einblicke, lassen sich die somit ermittelte Erfahrungen wieder als Anforderungen formulieren, um die bestehenden Anforderungen zu verfeinern oder zu ergänzen.

Bibliographie

[1] L. W. Anderson und D. R. Krathwohl, Hrsg., *A Taxonomy for Learning, Teaching, and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives*, Complete ed. New York: Longman, 2001.

[2] M. T. H. Chi und R. Wylie, „The ICAP Framework: Linking Cognitive Engagement to Active Learning Outcomes“, *Educational Psychologist*, Bd. 49, Nr. 4, S. 219–243, Okt. 2014, doi: 10.1080/00461520.2014.965823.

[3] G. Costa und M. Ribaudo, „Designing a Serious Game for Cybersecurity Education“, *Software Engineering for Games in Serious Contexts*. Springer Nature Switzerland, Cham, S. 265–290, 2023. doi: 10.1007/978-3-031-33338-5_12.

[4] K. M. L. Cooper und A. Bucchiarone, Hrsg., *Software Engineering for Games in Serious Contexts*. Cham: Springer Nature Switzerland, 2023. doi: 10.1007/978-3-031-33338-5_12.

[5] T. Espinha Gasiba, K. Beckers, S. Suppan, und F. Rezabek, „On the Requirements for Serious Games Geared Towards Software Developers in the Industry“, in *2019 IEEE 27th International Requirements Engineering Conference (RE)*, Jeju Island, Korea (South): IEEE, Sep. 2019, S. 286–296. doi: 10.1109/RE.2019.00038.

[6] J. Eckstein, J. Bergin, und H. Sharp, „Patterns for Active Learning“, in *Proceedings of PLOP*, 2002.

[7] CTFtime team, „What Is Capture The Flag?“. Zugegriffen: 24. Februar 2025. [Online]. Verfügbar unter: https://ctftime.org/ctf-wtf/

[8] A. Siami Namin, Z. Aguirre-Muñoz, Texas Tech University, und K. Jones, „Teaching Cyber Security through Competition An Experience Report about a Participatory Training Workshop“, in *7th Annual International Conference on Computer Science Education: Innovation & Technology (CSEIT 2016)*, Global Science & Technology Forum (GSTF), Okt. 2016. doi: 10.5176/2251-2195_CSEIT16.39.

[9] K. Leune und S. J. Petrilli, „Using Capture-the-Flag to Enhance the Effectiveness of Cybersecurity Education“, in *Proceedings of the 18th Annual Conference on Information Technology Education*, Rochester New York USA: ACM, Sep. 2017, S. 47–52. doi: 10.1145/3125659.3125686.

[10] MITRE Corporation, „Common Weakness Enumeration - CWE Version 4.16“. Zugegriffen: 25. Februar 2025. [Online]. Verfügbar unter: https://cwe.mitre.org/data/published/cwe_v4.16.pdf

[11] „OWASP Top 10:2021“. Zugegriffen: 25. Februar 2025. [Online]. Verfügbar unter: https://owasp.org/Top10/de/

[12] „OWASP Top Ten | OWASP Foundation“. Zugegriffen: 25. Februar 2025. [Online]. Verfügbar unter: https://owasp.org/www-project-top-ten/

[13] „A01:2021 – Mangelhafte Zugriffskontrolle - OWASP Top 10:2021“. Zugegriffen: 26. Februar 2025. [Online]. Verfügbar unter: https://owasp.org/Top10/de/A01_2021-Broken_Access_Control/

[14] „Faq - Reddit.Com“. Zugegriffen: 26. Februar 2025. [Online]. Verfügbar unter: https://web.archive.org/web/20201127015655/http://www.reddit.com/wiki/faq#wiki_what_does_the_name_.22reddit.22_mean.3F

[15] „CWE - CWE-425: Direct Request ('Forced Browsing') (4.16)“. Zugegriffen: 25. Februar 2025. [Online]. Verfügbar unter: https://cwe.mitre.org/data/definitions/425.html

[16] „CWE - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor (4.16)“. Zugegriffen: 25. Februar 2025. [Online]. Verfügbar unter: https://cwe.mitre.org/data/definitions/200.html

[17] „CWE - CWE-862: Missing Authorization (4.16)“. Zugegriffen: 25. Februar 2025. [Online]. Verfügbar unter: https://cwe.mitre.org/data/definitions/862.html

[18] V. Wanick, J. Stallwood, und G. Xavier, „Future Directions in Games for Serious Contexts: A Conversation About Transferability“, *Software Engineering for Games in Serious Contexts*. Springer Nature Switzerland, Cham, S. 137–153, 2023. doi: 10.1007/978-3-031-33338-5_7.

[19] S. Kirginas, „User Experience Evaluation Methods for Games in Serious Contexts“, *Software Engineering for Games in Serious Contexts*. Springer Nature Switzerland, Cham, S. 19–42, 2023. doi: 10.1007/978-3-031-33338-5_2.

[20] R. Raman, S. Sunny, V. Pavithran, und K. Achuthan, „Framework for Evaluating Capture the Flag (CTF) Security Competitions“, in *International Conference for Convergence for Technology-2014*, Pune, India: IEEE, Apr. 2014, S. 1–5. doi: 10.1109/I2CT.2014.7092098.